26. (Previously Presented) The method of claim 24 wherein a proof of work POW is (w, p, m)-feasible if there exists a prover P with memory resources bounded by m such that with an average of w steps of computation in the time interval $[t_s, t_c]$, the prover can cause the verifier V to accept with probability at least p.

27. (Previously Presented) The method of claim 24 wherein a proof of work POW is sound, if, for some w, POW is (w, l, poly (l))-feasible, where l is a security parameter.

28. (Previously Presented) The method of claim 24 wherein a POW may be regarded as efficient if the verifier performs substantially less computation than the prover.

REMARKS

Reconsideration and allowance of the claims pending in the application are requested.

Claims 1 – 28 are pending in the application.

Claim 4 has been objected to because of minor informalities.

Claims 1-4 have been rejected under 35 USC 102(e) as being anticipated by USP 6,005,938 to Banker, issued December 21, 1999, filed December 16, 1996 (Banker).

Claims 5-7, 12-15, 17 and 23 have been rejected under 35 USC 102(e) as being anticipated by USP 6,212,634 B1 to D. F. Geer Jr., et al., issued April 3, 2001, filed November 15, 1996 (Geer).

Claims 24-28 have been rejected under 35 USC 102(e) as being anticipated by USP 6,237,097 B1 to Frankel, of record (Frankel).

Claims 8, 9, and 11 have been rejected under 35 USC 103(a) as being unpatentable over Geer as applied to claim 5 above, and further in view of USP 6,549,210 B1 to Van Hook et al. (VanHook), of record.

Claims 10 and 18 have been rejected under 35 USC 103(a) as being unpatentable over Geer as applied to claims 5 and 13 above and further in view of USP 6,662,167 B1 to Xiao, of record (Xiao).

Claims 16 and 19-21 have been rejected under 35 USC 103(a) as being unpatentable over Geer as applied to claim 13 above and further in view as applied to USP 5,768,385 to Simon, of record (Simon).

Claim 22 has been rejected under 35 USC 103(a) as being unpatentable over Geer as applied to claim 13 above and further in view of USP 5,768,385 to Simon, of record

Applicants attorney thanks Primary Examiner S. Zia and Examiner A. K. Moorthy for the courtesy of a personal interview conducted with Applicants' attorney on November 21, 2005 in which A. Juels , an inventor and M. Rosenberg, Patent Counsel for the assignee participated by telephone. At the interview, the concept of a POW was discussed. The differences between client puzzles and POWs was discussed. The Examiners pointed out sections of application to incorporate into the preamble and body of the independent claims 1 and 5. An amendment of the independent claims to include distribution of the POW as a POW would overcome the cited art. Applicants indicated a RCE would be prepared and filed to incorporate the results of the interview into the claims which would be subject to a new search.

Before responding to the rejection and having previously distinguished Frankel, of record; Van Hook, of record; Xiao, of record, Simon, of record and Puhl, of record from the claimed subject matter of Jakobsson in the amendment filed June 5, 2005, applicants would like to distinguish Banker and Geer from the claimed subject, as follows:

A. Banker discloses a technique for preventing replay attacks on digital information distributed by network service providers. At the beginning of a subscription period for a service, a network service provider sends entitlement messages to the subscriber which provide the subscriber for the service with a session key and authorization information. The authorization information specifies a service and a period of time. When an encrypted instance of a service is distributed on the network, it is accompanied by a series of entitlement control messages. Each of the messages includes a value which can be used with the session key to obtain a control word for decrypting the encrypted instance and a time specifier. The subscriber equipment which decrypts the instance of the service does so only if the time specifier in the entitlement control message specifies a time within the time period specified by the authorization information.

Banker fails to disclose a POW as disclosed and claimed. Banker discloses a CATV system protecting digital information that is provided to users of a network by network service providers and more specifically concerns protecting the information against the class of attacks termed replay attacks, that is, attacks which work by replaying decryption information that the user received while he was subscribed to a service to decrypt information from the service after he has dropped his subscription

Moreover, Banker does not relate to a POW. A POW is a protocol between two or more participants in which one or more participants can determine that one or more, potentially overlapping, participants performed some tasks, where (a) it is known what approximate computational effort such tasks take; (b) the computational effort is large enough to easily make it a potential bottleneck if one participant attempts to perform too many such tasks; (c) it takes a substantially smaller effort to generate an instance task than to solve it, and (d) it takes a substantially smaller effort to verify the solution to a task than to solve it. Here, substantially smaller is used to mean that the task is not likely to become a potential bottleneck to the party performing the task, given similar number of tasks for this party to generate/verify as for another party to solve, and where the solving effort may be a bottleneck.

Further, Banker does not distribute among CATV subscribers a computational task among a plurality of entities for execution within a specified interval of time as a POW.

Nor, does the CATV service provider receive the POW relating to said task from one of said plurality of entities and uses the POW to accomplish the task.

Still further, the minting of public and private keys between a CATV service provider and a service subscriber in Banker does not equate to minting coins in Jakobsson for an electronic payment system where the minting operation is distributed by an entity among a plurality of other entities in a manner that maintains privacy in the minting operation, and one of the plurality of entities provides a POW to the distributing entity to accomplish the minting operation.

Summarizing, there is no disclosure in Banker of (i) a POW or (ii) distributing a computational task among a plurality of entities and (iii) receiving a POW from one of the entities to accomplish the computational task or (iv) simplifying a minting operation by (v) partitioning the minting operation into a plurality of sub-tasks among a plurality of entities and (vi) receiving a POW from one of the entities to accomplish the minting operation.

B. Geer discloses a system for certifying authorizations includes an authorizing computer and an authorized computer interconnected by a computer network. The authorizing computer creates a public key pair comprising a new public key and a new private key, and creates an authorization certificate that certifies that a holder of the authorization certificate is authorized to perform an action referred to in the authorization certificate. The authorization certificate includes the new public key. The authorizing computer causes the authorization certificate and the new private key to be transmitted to the authorized computer. The authorized computer receives the authorization certificate and the new private key and decrypts messages using the new private key as evidence that the authorized computer has obtained the authorization certificate legitimately.

Geer discloses the authorized computer proves itself to the authorizing computer by sending a public key certificate identifying the user of the authorized computer and the user's public key. Geer fails to disclose an entity (i) distributing a computational task among a plurality of entities for execution within a specified interval of time as a POW; (ii) receiving the POW

relating to said task from one of said plurality of entities; and (iii) using the POW to accomplish the task.

Moreover, Geer discloses the authorizing computer deals one-on-one with an authorized computer and not a plurality of computers as in Jakobsson. Geer discloses a minting operation for public and private keys. In contrast, Jakobsson discloses minting coins by partitioning the minting operation into sub-tasks for distribution among a plurality of entities and receiving a POW from one entity for use in accomplishing the minting operation

Summarizing, Geer fails to disclose (i) a POW or (ii) distributing a computational task among a plurality of entities or (iii) distributing a minting operation among a plurality of entities after partitioning the task into sub-tasks and receiving a POW from one entity used in accomplishing the minting operation.

C. Frankel discloses a distribution system for secret information. Frankel does not disclose a POW for the reason indicated in the amendment filed June 6, 2005.

Summarizing, the rejection of claims 1-4 based on Banker; claims 5-7, 12-15, 17 and 23 based on Geer; claims 24-28 based Frankel under 35 USC 102 (e) is without support in the cited art. Withdrawal and allowance of the rejected claims are requested. Likewise, the rejection of dependent claims 8-10; 16, 18-21 and 22 under 35 USC 103 (a) based on Geer in view of secondary art is without support in the cited art. Withdrawal and allowance of the rejected claims are requested.

Now turning to the rejection, applicants respond to the indicated paragraph of the Office Action, as follows:

Paragraphs 1/4:

The Examiner's statements are noted.

Regarding Paragraph 5:

Claim 4 has been amended to depend upon claim 2 and overcome the lack of antecedent.

Paragraph 6:

Claims 1-4 include features not disclosed in Banker and overcome the rejection under 35 USC 102 (e), as follows:

A. Claim 1:

(i) "distributing a computational task among a plurality of entities for execution within a specified interval of time as a POW;"

Banker at col. 4, lines 37-53 discloses a service provider providing an authorization entitlement message (AEMM) to a sole service subscriber. The AEMM includes validation data specifying the period of time for which the AEMM is valid. There is no disclosure in Banker of distributing the AEMM to multiple subscribers for performing a computational task with in a specified period, as described Jakobsson at page 3, lines 14-23. Banker fails to disclose elements of item (i)

(ii) "receiving the POW relating to said task from one of said plurality of entities; and using said POW to accomplish said task."

There is no description in col. 4, lines 37-53 or in col. 5, lines 6-62 or in Figs 3 and 5 of Banker showing the secure processor of the subscriber returning a signal, much less a POW, to the service provider relating to a computational task distributed to the service subscriber.

Banker fails to disclose a POW or the elements of claim 1. The rejection of claim 1 under 35 USC 102 (e) based on Banker is without support in the cited art. Withdrawal of the rejection and allowance of claim 1 are requested.

B. Claim 2:

The method of claim 1 further comprising using said POW to accomplish a security goal.

Banker at col. 5, lines 6-62 discloses an entitlement control message (ECM) processed by the subscriber to decrypt a service instance associated with the ECM. There is no disclosure that the service instance is a POW or the service provider processing the ECM. In contrast, applicant at page 4, line 1. Banker fails to disclose the elements of claim 2.

C. Claim 3 has been canceled.

D. Claim 4 The method of claim 2 wherein said security goal involves restricting resource access by said one of said plurality of entities.

Banker at col. 6, lines 28-54 discloses employing the invention in CATV services providing instances of service to subscribers using ECMs. In contrast, applicant discloses limiting resource access using POWs, a computational task. Banker fails to disclose POWs for limiting access to resources, and the elements of claim 4.

Summarizing, Claim 1, 2 and 4 are distinguishable from Banker by the failure of Banker to (i) disclose POWs, (ii) distributing POWs to a plurality of entities by an imitating entity and (iii) using the POWs by the initiating entity for security goal purposes. The rejection of claims 1-4 is with out support in the cited art. Withdrawal of the rejection under 35 USC 102 (e) and allowance of claims 1 -4 are requested.

Paragraph 7:

Claims 5-7, 12-15, 17 and 23 include features not disclosed in Geer and overcome the rejection under 35 USC 02 (e), as follows:

A. Claims 5 and 13:

(i) "partitioning a minting operation into a plurality of sub-computational tasks;"

Geer at column 3, line 55 continuing to col. 4, line 56 discloses minting public and private keys for transaction purpose in an electronic payment system. There is no disclosure of minting coins for an electronic payment system as described in Jakobsson at page 10, line 3-12. Geer also fails to disclose partitioning the minting operation into a collection of tasks and distributing the tasks to a large group of untrusted computational devices.

(ii) "distributing one of said plurality of sub-computational tasks to one of a plurality of entities;"

Geer at column 3, line 55 continuing to col. 4, line 56 and in Figs 2A and 2B discloses a transaction executed between a merchant and a customer via an authorized computer operated by the merchant and an authorizing computer operated by the merchant. Applicants can find no disclosure in Geer relative to distributing sub computational task to one of a plurality entities or merchants.

(iii) "receiving a POW from said one of said plurality of entities; and using said POW to accomplish said minting operation."

Applicants can find no disclosure in Geer at column 3, line 55 continuing to col. 4, line 56 relative to this claimed feature as shown in Fig. 3 of Jakobsson.

Geer fails to disclose the subject matter of claims 5 and 13. Withdrawal of the rejection under 35 USC 102 (e) and allowance of claims 5 and 13 are requested.

B. Claims 6 and 14:

(i) "The method of claim 5 further comprising using said POW to accomplish a security goal."

Geer uses public and private keys to achieve a security goal. In contrast, applicants use the POW to achieve security goals as described in Jakobsson at page 8, line 16 - 23.

Geer fails to disclose the subject matter of claims 6 and 14. Withdrawal of the rejection under 35 USC 102 (e) and allowance of claims 6 and 14 are requested

C. Claims 12, and 15:

Claim 7 has been canceled.

(i) "The method of claim 5 wherein said minting operation includes identifying valid solutions that hash to a predetermined image and wherein said POW represents a valid solution."

Geer at col. 5, line 52 continuing to col. 6 , line 3 discloses a certificate minted by the smart card at the authorizing computer is a file structure having a set of "criticals" and a set of "extensions." Applicants can find no disclosure in the cited reference to a minting operation which includes identifying valid solutions of the operation that hash to a predetermined image and wherein said POW represents a valid solution, as described in Jakobsson at page 10, lines 13-14.

Geer fails to disclose the subject matter of claims 12 and 15. Withdrawal of the rejection under 35 USC 102 (e) and allowance of claims 12 and 15 are requested

D. Claim 17:

(i) "The method of claim 15 wherein said predetermined number of valid solutions hash to a portion of said target value."

Claim 17 is distinguishable from Geer for the same reasons indicated above in the consideration of claim 5.

E. Claim 23:

(i) "The method of claim 13 further comprising verifying said POW."

The cited reference discloses certificates minted by a smart card. Applicants can find no disclosure in Geer relative to verifying a POW in a minting operation for coins.

Geer fails to disclose the subject matter of claim 23. Withdrawal of the rejection under 35 USC 102 (e) and allowance of claim 23 are requested.

Paragraph 8:

Claims 24-28 include features not disclosed in Frankel and overcome the rejection under 35 USC 102 (e), as follows:

A. Claim 24:

(i) "generating a computational task for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate useful and verifiable correct computation"

Frankel, at col. 10, lines 38-48, discloses servers generating and verifying randomized polynomials for verifying shares in a secret key assembled by a group of computers. All servers having to check shares to see whether local server shares match public shares. The cited text does not describe generating a POW to accomplish a separate, useful and verifiable correct computation.

(ii) "distributing the computational task for execution among a plurality of server entities;"

Frankel, at col. 10, lines 49-67, describes proving correctness of verification shares. Each server generates random polynomials. The server distribute the shares in these polynomials and broadcasts verification shares. Each server verifies its received polynomial shares, and the received verification shares. Col. 10, lines 49-67. The cited text discloses a verification operation and not a computational operation.

(iii) "using said POW to verify and accomplish said computational task."

Frankel, at col. 10, lines 49-67, describes proving the correctness of verification shares. Frankel discloses verifying secret shares with verification shares and fails to disclose a POW by which a prover demonstrates to a verifier that a certain amount of computation work has been performed in a specified interval of time. The matching of secret shares and verification shares does not disclose or suggest a POW accomplishing a computational task. Frankel does not disclose or suggest using a POW to accomplish a computational task for a minting operation which minimizes effort by reusing POWs.

Frankel fails to disclose the limitations of claim 24, as described above and without such disclosure, there is no support for the rejection of claim 24 under 35 US 102(e). Withdrawal of the rejection and allowance of claim 24 are requested.

B. Claim 25:

Frankel, at col. 12, line 51 to col. 13, line 29, describes proof of knowledge of corresponding representations where a prover proves that it knows the values of corresponding representations. The cited text does not describe or suggest a POW having a hardness by a Prover and Verifier performing coin flips of at most w steps of computation in a time interval,. Claim 25 further limits claim 24 and further distinguishes claim 24 from the cited art. Withdrawal of the rejection and allowance of claim 25 are requested.

C. Claim 26:

Frankel, at col. 13, line 60 to col. 14, line 19, describes determining whether a previously computed value N is the product of two prime numbers. Frankel does not disclose determining if a proof of work is feasible if a Prover with an average of w computation steps in a time interval can cause a Verifier to the proof within a probability p. Frankel does not address the problem of identifying a feasible proof of work, but is directed to verifying shares of a secret key.

D. Claim 27:

Frankel, at col. 13, lines 60 to col. 14, line 19, fails to disclose the limitations of claim 27 on the same basis as the cited text failed to describe or suggest claim 26.

E. Claim 28:

Frankel, at col. 14, line 37 to col. 15, line 22, describes key generations for small public key. The cited text does not describe a POW or an efficient POW which reduces the work of a verifier by re-cycling POWs.

Summarizing, claims 24-28 relate to qualities of POWs whereas Frankel is directed to RSA key generation. The rejection of claims 24-28 under 35 USC 102e is without support in the cited art.

Paragraph 9:

Claim 8, 9 and 11 include limitations not disclosed or suggested in Geer in view of Van Hook, of record, and overcome the rejection under 35 USC 103 (a), as follows: follows:

A. Claims 8 & 9:

(i) "The method of claim 6 wherein said predetermined image comprises a range of images. and wherein all images within said range of images have a predetermined number of least significant bits in common."

Van Hook does not supply the missing elements in Geer relative to predetermined images comprising a range of images having a predetermined number of least significant bits in common. Van Hook appears to use hash functions of a different type than is used in cryptography. There are two types of computation known as hashing. The one that Van Hook relates to is not collision resistant, and is not hard to invert. The Jakobsson hash functions are collision resistant and hard to invert. Van Hook cannot practice his invention with a cryptographic hash function. To do so, would render his technique meaningless. Whereas Jakobsson could distribute any type of hashing Function. Moreover, finding partial hash collisions is not meaningful in the context of hash functions of the type disclosed by Van Hook.

In particular, Van Hook, at col. 9, lines 55-67, discloses hashing an index of coordinate values descriptive of an image where the hashed index value is used to map the memory locations in main memory. The locations are referred to by (s) "and (t) coordinates". The hashed index enables coordinates varying in only a few bits to be mapped to different locations in a cache memory. In contrast, Applicants, at pg. 11, lines 8-12, disclose an entity transmits a hash function to be used in identifying collisions within a predefined search space for pre-images that have a range of images whose "t" least significant bits have the value "s".

Van Hook hashes an index of coordinates for an image location and fails to disclose hashing the coordinates of a range of images that map to a single image.

Van Hook, at col. 11, line 13-25, discloses a process for cache index hashing for an (s) coordinate that is fed into first and second portions on a (t) address is fed into first and second portions. The division of coordinates can be based on some number that most or least significant bits or any other suitable scheme. The cited text does not disclose or suggest images within a range of images have a predetermined number of least significant bits in common.

Summarizing, applicants describe a linking operation that identifies valid solutions that hash to a range of images for a predetermined image. Van Hook does the opposite of Jakobsson by reducing the likelihood that adjacent addresses will match the map to the same cache region. Moreover, the Examiner has not demonstrated in any respect a motivation or reasonable expectation of success in combining Van Hook with Geer to implement a computational effort invested in a proof of work for accomplishing a minting operation. Finally, Geer and Van Hook fail to disclose all of the limitations of claim 8 and 9.

The rejection of claims 8 and 9, under 35 USC 103(a) is not supported in the cited art. Withdrawal of the rejection and allowance of claims 8 and 9 are requested.

B. Claim 11:

Claim 11 further limits claims 5 and 6 in overcoming the rejection under 35 USC 103 (a)., and is patentable on the same basis as claim 5.

Paragraph 10:

Claims 10 and 18 include limitations not disclosed or suggested in Geer, in view of Xaio, of record, and overcome the rejection under 35 USC 103 (a) as follows:

A. Claims 10 & 18:

Xiao does not supply the missing limitations in Geer. Xiao, at col. 2, lines 26-53 discloses the parameters for real-world scheduling/sequencing to accommodate different conditions and able to adapt to changes. Applicants can find no disclosure in Xiao relating to searching a different solution search space for valid solutions, as described in the

specification at pg. 11, line 20 continuing to pg. 12, line 5. The scheduling/sequencing problems and evolutionary computation used in resolving those manufacturing scheduling problems, does not disclose or suggest sub-task searching different solution search space for valid solutions. Without such disclosure, there is no basis for a worker skilled in the art to implement claims 10 and 18. the rejection of claims 10 and 18 under 35 USC 103(a) fails for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested.

The motivation to modify Geer by the teachings of Xiao to produce a near optimal or optimal sequence of products for manufacture does not enable a worker skilled in the art to implement a minting operation in a computational effort invested in a POW. The rejection of claims 10 and 19, based on 35 USC 103(a) is without support in the cited art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested.

Paragraph 11:

Claims 16 and 19-21 include features not disclosed or suggested in Geer in view of Simon, of record and overcome the rejection under 35 USC 103 (a), as follows

Simon fails to disclose the missing limitations in Geer. Simon, at col. 8, lines 65 to col. 9, line 15, discloses public keying encryption and the use of message authentication codes to ensure that messages between parties are not tampered with by someone other than the sender. Applicants can find no disclosure in Simon relating to using a suitable hash function and string concatenation, including a secret value, for generating a coin to be minted, as described in the specification at pg. 13, lines 3-14.

A worker skilled in the art would not be motivated to modify Geer with Simon to implement a method of accomplishing a minting operation using a computational effort invested in a POW. Without such motivation or reasonable expectation of success, and the failure of the cited references to describe all of the claim limitations, there is no basis under 35 USC 103(a) for the rejection of claim 16 and 19-21.

Withdrawal of the rejection and allowance of claims 16 and 19-21 requested.

Paragraph 12:

A. Claim 22:

Claim 22 includes limitations not disclosed in Geer, in view of Puhl, of record, and overcome the rejection under 35 USC 103 (a), as follows:

(i) "he method of claim 19 wherein said hash is of a concatenation of a solution and a value generated using said secret value."

Puhl fails to disclose the missing limitation in Geer. Puhl, at col. 17, lines 24-42, discloses storing secret keys and member certificates in a wireless identity module software token. The member keys are protected by pass phrase information. The information is concatenated with a secret value for the device and run through a secure hash in order to generate encryption/encryption key for use in protecting the user's private key. In contrast, applicants at page 13, lines disclose a hash function is concatenated with a secret value "r" specific to each coin to be minted. The computation performed aids in the successful completion of the task of finding the requisite number of pre-image values that hash to a specific range of images for the purpose of minting coins. Puhl discloses hashing for generating encryption/encryption keys and not for the purpose of minting coins.

A worker skilled in the art would not be motivated to modify a method of modeling an enterprise, via a wireless electronic commerce system, to implement a minting operation having privacy using a hash operation and a secret value. Further, the Examiner has not demonstrated any reasonable expectation of success for such a combination to implement the method of claim 22. The rejection of claim 22 is without support in the cited art. Withdrawal of the rejection and allowance of claim 22 are requested.

CONCLUSION

Applicants have established the cited art does not disclose or suggest a computational task distributed among a plurality of entities for generation of a Proof of Work (POW) and using one of the POWs in accomplishing the computational task. Accordingly, the rejection of claims 1, 2, 4-6, 8-28 under 35 USC 102(e) or 35 USC 103(a) is without support in the cited art. The application is in condition for allowance. Entry of the amendment , allowance of the claims, and passage to issue of the case are requested or alternatively, entry of the amendment for purposes of appeal is requested.

AUTHORIZATION:

The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. 13-4503, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4503, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,

MORGAN & FINNEGAN, L.L.P.

Dated: November 23, 2005

By: Joseph C. Redmond

Joseph C. Redmond, Jr., Reg. No. 18,753
Telephone: (202) 857-7887
Facsimile: (202) 857-7929

CORRESPONDENCE ADDRESS:
Morgan & Finnegan L.L.P.
3 World Financial Center
New York New York